Zeichner Risk Analytics – Comments on The Effects on Broadband Communications Networks of Damage To or Failure of Network Equipment or Severe Overload. (FCC 47 CFR Chapter I, [PS Docket No. 10-92; FCC 10-62])

Updating and reinvigorating the nation's national security & emergency preparedness (NS/EP) policy is essential for any discussion involving the security and reliability of critical broadband communications. The Federal Communications Commission, in close collaboration with the Administration and key industry stakeholders should fully define national priorities that constitute a new, long-lasting NS/EP agenda.

EXECUTIVE SUMMARY

This document provides Zeichner Risk Analytic's ("ZRA") comments on the "Effects on Broadband Communications Networks of Damage To or Failure of Network Equipment or Severe Overload" presented as a Proposed Rule in the Federal Registrar Volume 75, Number 90 on Tuesday May 11th, 2010. ZRA is grateful for the opportunity to comment on what we believe is a critical discussion of national interest.

Any effort to improve the survivability of broadband communication networks, reduce network vulnerabilities, and the evaluation of sufficient redundancies must be based on a foundational policy reflecting national priorities. Just as National Security Decision Directive 97 and Executive Order 12472 defined these priorities for telecommunications networks in the mid-1980's, a similar national security & emergency preparedness ("NS/EP") framework must be developed covering broadband communications networks and the Internet; this NS/EP foundation must be carefully designed by key Administration stakeholders, including the Department of Homeland Security (DHS). Additionally, a new NS/EP framework can only be established in close collaboration between government officials and owners and operators of essential broadband infrastructure in the private sector.

DISCUSSION

Formed in 2001, ZRA consults with institutions in both the public and private sectors to manage strategic, organizational, and corporate governance demands. Over the past nine years, we have increasingly witnessed a growing demand for global leadership around challenges associated with NS/EP telecommunications and information systems. Given our perspective on strategic challenges, we believe that any discussion on broadband survivability must consider NS/EP priorities, such as those memorialized in EO 12472, as amended, and subsequent doctrine created by the National Communications System and the National Communications Center.

Immediately after the break-up of "Ma Bell" In the mid-1980s, senior public and private leaders negotiated and memorialized priorities for the management of telecommunications resources to ensure national security and emergency preparedness. Policy documents, including Presidential decision directives, executive orders, and Federal policy documents shifted national focus to five clear objectives:

1) Support for the vital functions of worldwide intelligence collection and diplomacy;
2) A reliable and enduring threat assessment capability;
3) Assured connectivity between the National Command Authority and military forces;
4) Support of military mobilization as directed by the President; and
5) Continuity of government and national leadership during and after crisis situations and recovery of critical functions following crisis situations.

Just as NSDD-97 and EO 12472 defined these critical objectives for management of NS/EP telecommunications resources, a similar policy stance needs to be made by the United States as it relates to broadband communication networks. The definition of national priorities is an essential step to galvanize the National approach towards the security, reliability, integrity and appropriate public-private governance. To this end, there are five critical areas that need to be addressed:

1) The reliance of critical infrastructure on the Internet and the position that will be taken by the United States to ensure uninterrupted operation of these functions;

2) Providing increased protection for sensitive national information, while simultaneously increasing government openness and transparency through the use of the Internet;

3) The dependence of the United States on broadband communication networks for intelligence and diplomacy functions;

4) The reliability and security of the Internet in support of the economic stability of the United States; and

5) The National priority placed on the Internet for both offensive and defensive military capabilities

By updating existing NS/EP policy objectives, including these five key areas, the Administration can better define a foundation for the technical and legal activities that will support the survivability and reliability of broadband communications.